

【ネットワーク LSI システム(藤野・熊木)研究室】

～ 特徴ある LSI アーキテクチャ&回路とセキュリティ&ネットワーク応用 ～

○研究紹介

大容量のメモリとマイクロプロセッサ等のロジック回路を、1チップの大規模集積回路(VLSI)上に実現した「システム LSI」は、さまざまな情報機器で利用される「小型低消費電力かつ高性能なシステムの実現」に必須の技術となっています。みなさんは、LSI の仕様が決定したら、ハードウェア記述言語 (HDL) で記述し、あとは LSI 設計 CAD を使って簡単にシステム LSI は作成できると考えているかもしれませんが、実際に低消費電力・高性能・低コスト・高信頼性などの要求を満足しようとすると、新しい特徴ある LSI アーキテクチャ&回路が必要となってきます。

当研究室では、以下のような LSI アーキテクチャ&回路の研究と応用を、教員(藤野, 熊木), 研究員(汐崎, Tuan), 研究補助員(浅川)と大学院生 11 名(来年度は 19 名予定)が、右記の外部機関と交流しながら行っています。

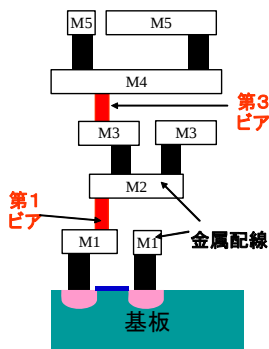
- (1) ビアプログラマブル LSI 設計<VP> ブリティッシュコロンビア大学
- (2) 耐タンパ LSI 設計&非接触電力転送<SCA> CREST プロジェクト (産業技術総合研究所, 名城大学)
- (3) マトリックス型超並列プロセッサ開発と応用<MX> ルネサスエレクトロニクス
- (4) 製造ばらつきを利用した固有 ID 生成技術<PUF> CREST プロジェクト (産業技術総合研究所, 名城大学)

研究ターゲットとしているアプリケーションは、現在、暗号化, 符号化, 乱数発生, 認証等を行っており, インターネット分野でますます重要になるネットワークセキュリティ技術の知識を修得できます。

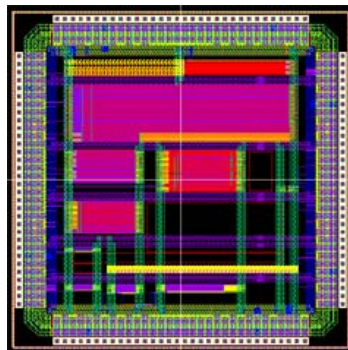
○研究テーマ説明図

(1) ビアプログラマブル LSI 設計 <VP>

LSI 製造工程でビア2~3層だけを、フォトマスクの不要な電子ビーム描画装置を使ってプログラムすることで、自由に回路論理を変更できる LSI。ASIC で回路論理を変更するために必要な1億円以上のマスクコストを削減でき、「世界で1つしかない LSI」を製造することが可能。LSI 試作実績のあるプログラマブルロジックの他、今年度よりプログラマブルアナログ回路も検討開始予定。

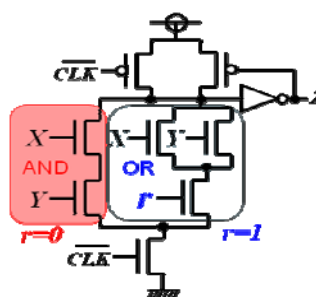


ウエハ断面構造

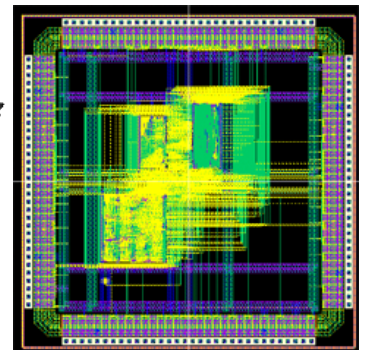


(2) 耐タンパ LSI 設計 &非接触電力転送<SCA>

暗号回路の動作中に、その消費電力をモニタすることで暗号鍵を推定する差分電力解析型サイドチャネル攻撃がセキュリティ上脅威となっている。このような攻撃から暗号回路を守る設計技術が「耐タンパ LSI 設計」である。当研究室オリジナルの乱数を用いて消費電力を均一化するドミノ RSL 回路を用いた DES 暗号回路を設計し耐タンパ性を評価している。

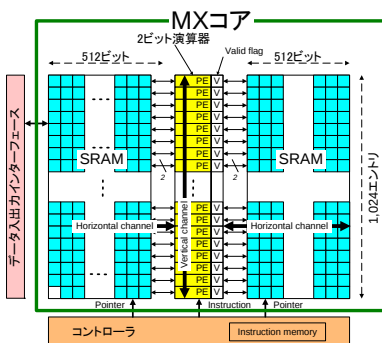


ドミノ型 RSL ゲート



(3) マトリックス型超並列プロセッサの開発と応用 <MX>

最大 1,024 並列のデータ処理能力を誇るモバイル機器向け LSI の開発とその応用を行っている。現在は暗号化, 乱数生成, 物体検出, 及びネットワークアプリケーション等の高速化について研究中。また、超小型マイコンボードを用いたアプリケーション開発も行っている。今年度から発足した研究テーマであり、メンバーの様々なアイデアを積極的に採用する方針である。



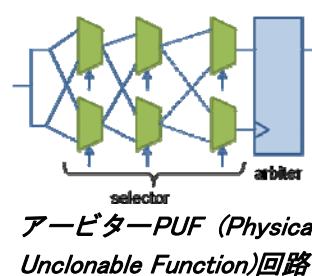
超並列 MX コア



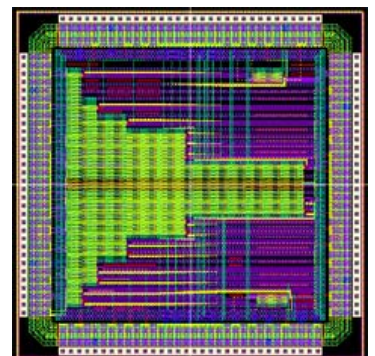
超小型マイコン実験ボード

(4) 製造ばらつきを使用した固有 ID 生成技術 <PUF>

IC カードや、LSI などの付加価値の高いデバイスを複製し不正使用するクローン攻撃を防止するためにはデバイスごとに固有の ID を持たせることが必要である。当研究室ではトランジスタチェーンの伝搬遅延時間の製造ばらつきを利用したアービター PUF を設計し、生成する ID 再現性と ID 衝突耐性を評価している。RFID の他将来は偽札偽造防止などにも役立つ可能性あり。



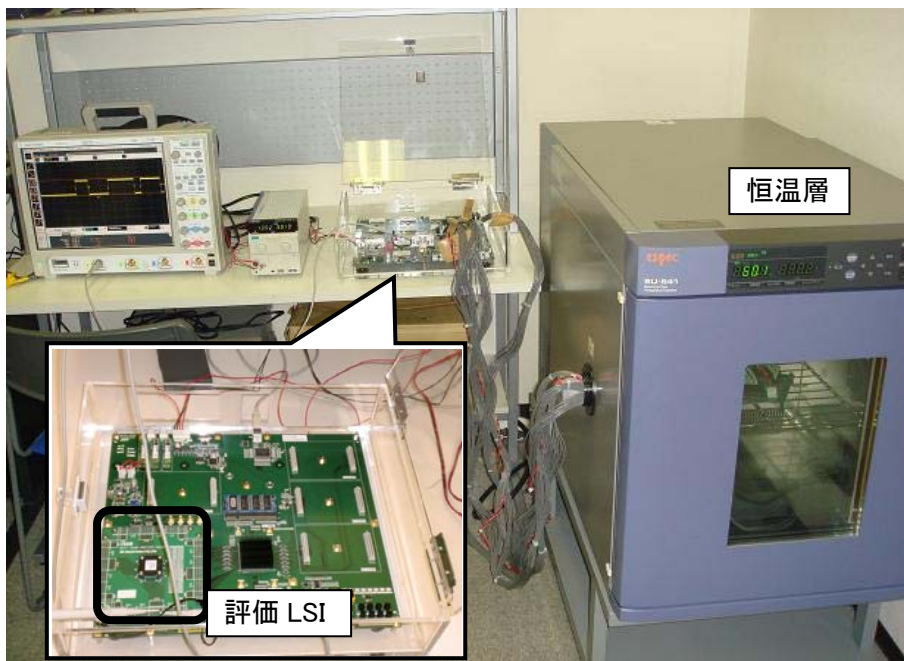
アービター PUF (Physical Unclonable Function) 回路



○使う研究設備

当研究室の大きな特徴は、**LSI を実際に作り評価する**というところです。過去1年で5種類の LSI を作成しました。今年5月に導入した LSI 設計用サーバー (Xeon 8Core CPU, 64GB Memory) 2台と設計ツール (ケイデンス, シノプシス, メンター) を駆使して, LSI を設計し, LSI 評価用 FPGA ボードを用いて評価します。

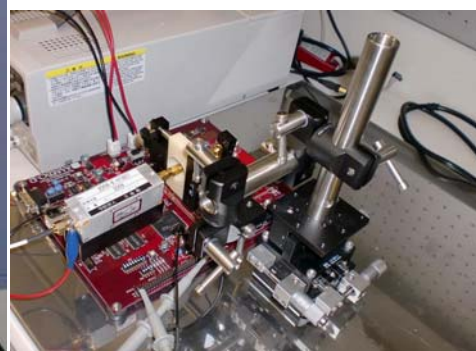
チップを作り, 評価していくことで C(C#), verilogHDL などのプログラミング, 電子回路, アナログ回路などの回路設計に関する実践的な技術を身につけていくことができます。



試作 LSI の評価設備



藤野・熊木研究室 LSI 設計サーバ

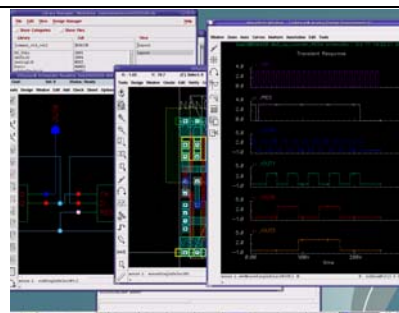


電磁波を用いたサイドチャネル攻撃実験設備

○卒業研究の進め方

配属学生は, 4 回生の夏前までに研究に必要なとなる知識を身につけ, 夏休みから本格的に研究を開始します。

輪講 (3 回生 ~ 4 回生)	LSI 設計技術に関する英文教科書 (「Introduction to VLSI Circuits and Systems」) と, ネットワークおよび暗号技術に関する技術書を, 毎週分担を決めて読み進めます。これにより, LSI 設計・ネットワーク技術の専門知識, 英語力, プレゼンテーション能力を養成します。
応用演習 (3 回生)	・ 本研究室の研究内容の紹介 ・ ノート PC 上でプログラミング環境を構築し C プログラミングの演習
院生ゼミ (4 回生前 期)	院生が協力して, 以下の LSI 設計&ネットワーク技術にかかわる以下の実習教育を, 2 回/週のペースで行います。 ・ 回路図作成, SPICE シミュレーション, 論理合成, レイアウト作成など一連の LSI 設計 CAD ツールを使った実習(右図) ・ verilogHDL による FPGA ボードプログラミング実装 実習教育は 6 月末で終了し, 7 月に卒研生の研究テーマ発表会を行い, 夏休みから, 各研究グループに分かれて, 院生と共同で卒業研究に取り組みます。



○さいごに

・工学部の学生, 特に電子・機械系の学生は, 企業に入って製品の研究開発に取り組むという学生が多いと思います。企業に入ると, 基本的には与えられたテーマを問題解決することが中心になりますので, 学生時代には, もっと自由な観点からエンジニアとしての基礎能力を養ってほしいと思います。具体的には, (1)新しい技術に対する好奇心をもつ, (2)自分のアイデアを持つ, (3)アイデアを実現する技術を持つ, (4)研究した技術を上手に発表する, という一連の流れを経験し, **日進月歩の電子情報技術分野で長くエンジニアとして生きていく力**を身につけてください。

・もちろん, エンジニアとしての基礎知識も重要です。当研究室は, LSI の HDL 設計~レイアウト設計, ネットワークプログラミング, 暗号技術など様々なテーマを扱っています。積極的に知識を吸収してください。

・ LSI の幅広い設計をやってみたい学生, 自分で LSI を設計して評価してみたい学生, ネットワークおよびネットワークセキュリティに興味ある学生, 自分の研究を国内外で発表したい学生, 歓迎します。

・本資料で当研究室に興味を持った方は, 是非 <http://www.ritsumei.ac.jp/se/re/fujinolab/> (公開サーバー) や <http://rh5pt200.bkc.ritsumei.ac.jp/wiki/> (研究室イントラネットサーバ) をアクセスしてみてください。メールや訪問による質問も歓迎ですので fujino@se.ritsumei.ac.jp または kumaki@fc.ritsumei.ac.jp に連絡してください。